Department of Justice

STATEMENT

OF

BARRY SABIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

"LEGISLATIVE HEARING ON H.R. 5304, THE 'PREVENTING HARASSMENT THROUGH OUTBOUND NUMBER ENFORCEMENT (PHONE) ACT'"

PRESENTED ON

NOVEMBER 15, 2006

Statement of Barry Sabin
Deputy Assistant Attorney General
Criminal Division, U.S. Department of Justice
Before the U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

Concerning

H.R. 5304, Preventing Harassment through Outbound Number Enforcement Act

November 15, 2006

I.

Introduction

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. It is my pleasure to appear before you to discuss H.R. 5304, the "Preventing Harassment through Outbound Number Enforcement Act (PHONE Act)." The United States Department of Justice supports Congressional action such as the PHONE Act to give law enforcement better tools to protect our citizens and our country from identity thieves, stalkers, and other criminals.

This bill targets a telephone calling practice known as "caller ID spoofing." Caller ID spoofing is the modification of caller ID information that causes the telephone network to display a number and other information on the recipient's caller ID display that is not the number of the actual caller.

Recently, caller ID spoofing services have become widely available, greatly increasing the number of people who have access to this tool to deceive others. By outlawing the misuse of caller ID spoofing, the PHONE Act, with modifications we will recommend today, can

improve the Department's ability to prevent crimes ranging from identity theft to harassment to pretexting.

II.

Caller ID Spoofing Is Being Used By Criminals To Commit Crimes Such as Identity Theft and to Invade Americans' Privacy.

Criminals can use caller ID spoofing to facilitate a number of crimes, including identity theft, harassment, privacy invasions, and even election fraud. Obviously, caller ID spoofing can help to hide the identity of a criminal, but it can go farther, actually defeating security measures that would have prevented a crime.

For example, caller ID spoofing can lend credibility to a criminal trying to trick an individual into giving up private information, such as a credit card number or social security number. By making it appear that the call is coming from a legitimate charity or bank, from a business's customer, or even from the office of a political campaign, a victim can be more easily fooled into giving up private information. For instance, a "pretexter" can call telephone companies pretending to be a subscriber and try to obtain the subscriber's private telephone records. If the caller ID information matches the subscriber's home telephone number, the pretexter can more easily gain access to those private records.

Caller ID spoofing can also create opportunities for abusers who could not otherwise contact their victims to reach into those victims' homes and further harass them. Misleading caller identification information could cause a victim to accept a call they would otherwise avoid or circumvent automatic call-blocking that would have prevented the harassing call from being connected.

Identity thieves, hackers, and other criminals might also use caller ID spoofing to circumvent security measures put in place by financial institutions, money transfer agents,

communication service providers, retailers, and restaurants. Such businesses sometimes use caller ID information as part of their fraud prevention measures as a way of confirming the identity of the caller. If the information fed into these systems is inaccurate, the security measures might be defeated and allow transactions or access to private information that would otherwise have not been permitted.

These concerns are not theoretical; we know that criminals are using these caller ID spoofing services to further their crimes today. Take, for instance, the case of James Turner Hopper, who pleaded guilty to several federal felony offenses involving identity theft. Hopper admitted that he obtained over 100 credit card numbers and associated identity information. He then placed calls to a money transfer agent and used the stolen credit card accounts to send money to himself and others. To make these calls, Hopper used a caller ID spoofing service in order to hide his true identity and to defeat internal security controls that would have disclosed that he was using other peoples' credit card numbers. Hopper was able to use this tactic more than 150 times while attempting to steal over $88,000. The United States District Court for the Southern District of California recently sentenced Hopper to 30 months in prison.

III.

Caller ID Spoofing Services Have Become Widespread and Readily Available to the Public.

Recent changes in technology have made caller ID spoofing much easier and less expensive, which has led to services that allow many who would otherwise lack the necessary technical sophistication or equipment to spoof caller ID to be able to do so from any telephone or Internet connection.

Widely available Voice-over-Internet-Protocol (VOIP) equipment can easily be

configured to populate the caller ID field with information of the user's choosing. Equipment owners can easily allow users to connect to their equipment through the Internet or through toll-free telephone numbers. Once connected to the spoofing service, users can connect to any other telephone and choose what telephone number they wish to transmit to their recipients. Numerous spoofing services exist today that allow anyone to change his or her caller ID information simply by placing a call through a toll-free number or by setting up the call through the Internet.

It is the widespread availability of these new services that has brought caller ID spoofing to the mainstream. While this development is relatively new, we are already seeing that the capability is being misused to facilitate crimes and could be used to hamper investigations.

Addressing the problem, of course, must be done carefully. We understand that modifications to caller ID information can be done for benign or even beneficial purposes. There are instances where caller ID information is modified to accurately reflect the calling party, such as in call forwarding or to meet the requirements of emergency telecommunications, such as E911. These are functions undertaken by the telephone companies where no one is misled as to the true calling party.

It has been claimed that caller ID spoofing serves to protect people's privacy. The PHONE Act already wisely preserves as an option for telephone users to use caller ID blocking, *i.e.*, preventing your number from being known. Simply put, the caller gets to make a choice about whether to reveal his or her number and the recipient gets to make a decision about whether to take the call.

Some have further suggested that, as an alternative to blocking caller ID information,

individuals would benefit from being able to modify caller ID information in order to provide alternative call-back information. While this could in some instances be a non-objectionable use, today, there is no requirement that providers of caller ID spoofing services make any effort to verify that the person requesting to place a call with altered caller ID has any right to use the number requested. This lack of verification provides opportunities for misuse.

Moreover, the widespread availability of caller ID spoofing services could complicate criminal investigations. For example, if kidnappers or terrorists were to use caller ID spoofing, law enforcement involved in fast-moving investigations could lose valuable time chasing down the wrong path.

IV.

H.R. 5304 Could Be Improved to More Effectively Combat the Harms Caused by Widely Available Caller ID Spoofing.

The Department is concerned with the widespread availability of caller ID spoofing services that present significant potential for abuse and hinder law enforcement's ability to investigate crime. We believe that this matter merits further study, and suggest that Congress consider whether a civil or criminal prohibition on caller ID spoofing services in appropriate circumstances would be warranted. We would be happy to work with the Subcommittee in exploring the issue further.

Overall, the bill supports the Department's efforts to combat the threats caused by caller ID spoofing. The Department was pleased to see that the scope of the bill includes both conventional telephone calling and many types of VOIP services. The drafters have also wisely recognized that, at times, it may be necessary to modify caller ID information in the course of authorized law enforcement and intelligence operations. Accordingly, the bill properly includes an exception for these legitimate law enforcement and intelligence

activities.

The Department has a number of other recommendations to clarify and strengthen the bill and to make it more effective.

A. The bill could be made more effective by creating a more graduated series of offenses rather than just a felony charge.

Subsection (a) would subject violators of the proposed law to fines or imprisonment or both, but creates only one felony offense. A felony is a very serious charge that carries heavy penalties that may not be proportional to the conduct at issue in every case. The drafters may wish to consider a more graduated series of offenses that would allow prosecutors to charge misdemeanor offenses in appropriate circumstances. For instance, felony penalties could be reserved for caller ID spoofing done in furtherance of another crime or tort, while other conduct could be reduced to the level of a misdemeanor offense. This could lead to greater use of the statute and more just results. Such an approach has been implemented in other federal criminal statutes such as 18 U.S.C. § 1030(c)(2)(B) (part of the Computer Fraud and Abuse Act) and 18 U.S.C. § 2701(b) (the criminal provision in the Electronic Communications Privacy Act). We suggest below language based on 18 U.S.C § 2701.

B. The bill could be made more effective by prohibiting attempts.

A prosecution should not depend on whether a criminal was successful in the object of his crime. Thus, if a call placed by a criminal attempting to mislead another does not connect for some reason, the criminal should be punishable as if the call had been completed. Such failures may occur, for example, where a service has blocked certain numbers, such as 911, or even for more mundane technical problems. Thus, we recommend that the bill punish attempts the same as the substantive offense.

C. The bill could be made more effective by incorporating technical changes.

The Department proposes a variety of changes that we believe will clarify the bill. Among other recommendations, these changes include a statement of jurisdiction, using technology-neutral terminology, and including a forfeiture provision. In a separate letter, we will pass on these suggestions to you, along with the Department's recommended edits to the bill.

V.

Conclusion

The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet this new challenge. Thank you for the opportunity to testify today and for your continuing support. I am happy to answer any questions you may have.